Recommended readings

- `LDAP for Rocket Scientists`
- Basic LDAP Concepts
- Understanding the LDAP Protocol, Data Hierarchy, and Entry Components

Openldap server documentation

Exercises are based on the `OpenLDAP` server implementation.

Related material at `http://www.openldap.org`.

What is LDAP anyway?

- **L**ightweight **D**irectory **A**ccess **P**rotocol
- Vendor independent
- IETF standard:

  Clients interact with servers using a directory access protocol

LDAP Server cli bind

Command	Result

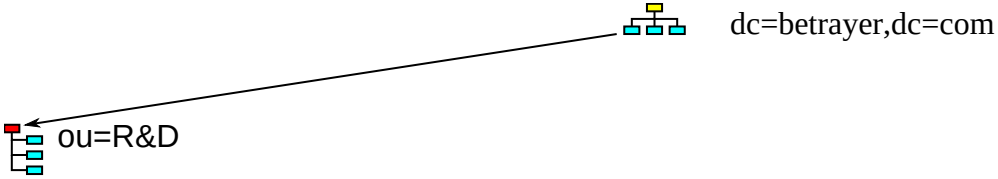
ldapsearch \
  -h localhost ❶ \
  -D "cn=admin,dc=betrayer,dc=com" ❷\
  -w password -x ❸\
  -b "dc=betrayer,dc=com" ❹\
  -s sub ❺ \
  -LLL ❻
	dn: dc=betrayer,dc=com ❶
	objectClass: top
	objectClass: dcObject
	objectClass: organization
	o: Betrayers heaven ❷
	dc: betrayer
	
	dn: cn=admin,dc=betrayer,dc=com ❸
	objectClass: simpleSecurityObject
	objectClass: organizationalRole
	cn: admin ❹
	description: LDAP administrator
	userPassword:: e1NT...dE53N1E= ❺

Document Information Tree (DIT)

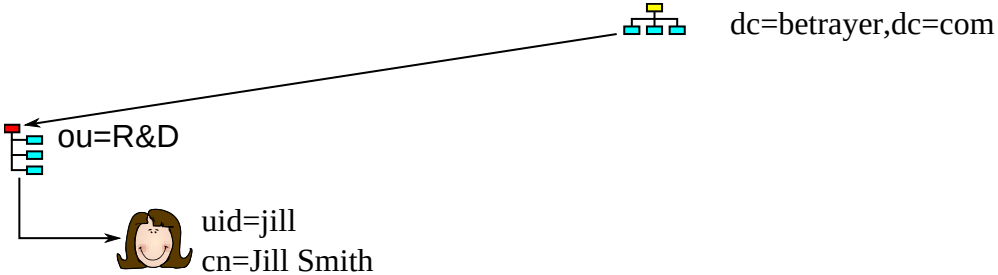
dc=betrayer,dc=com

ou=R&D

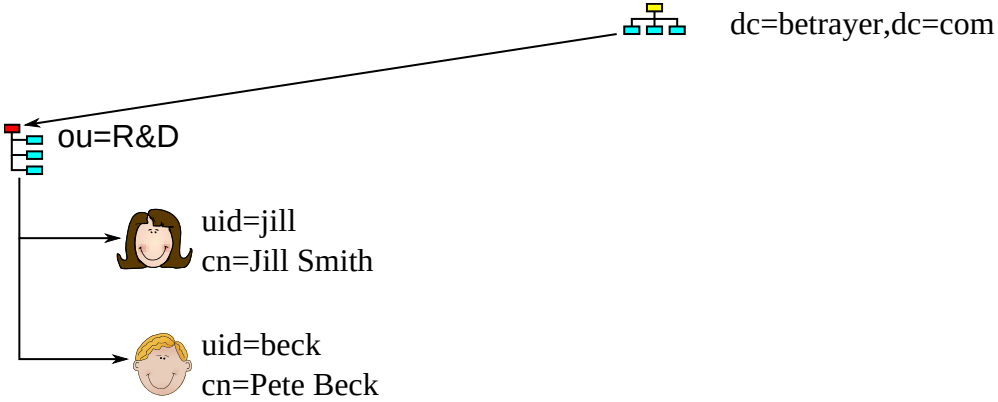
Document Information Tree (DIT)



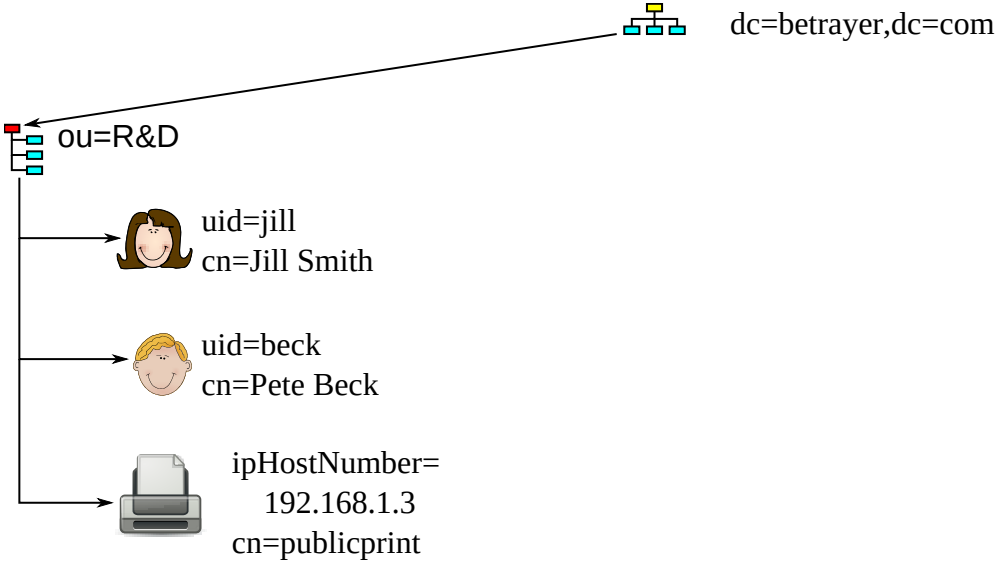
Document Information Tree (DIT)



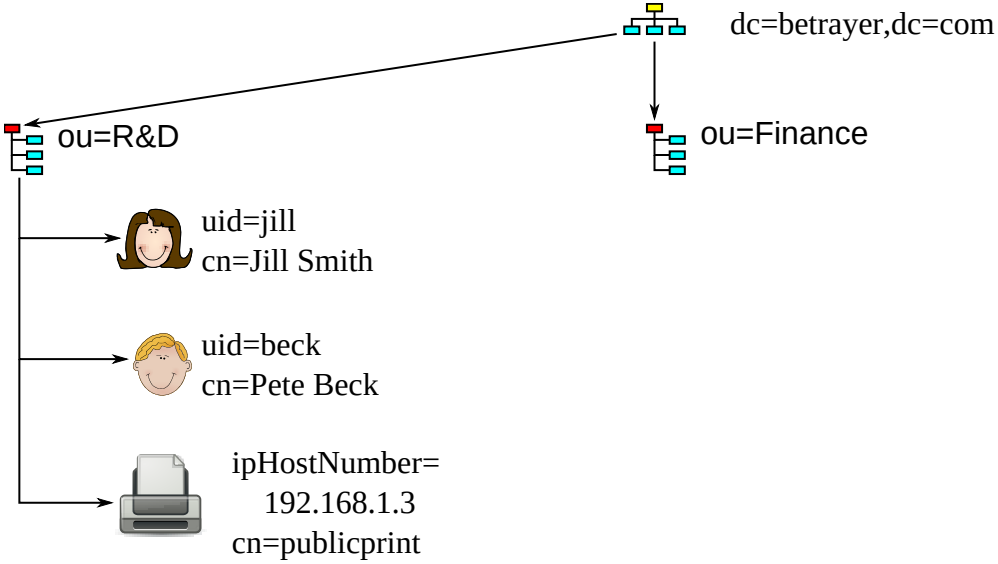
Document Information Tree (DIT)



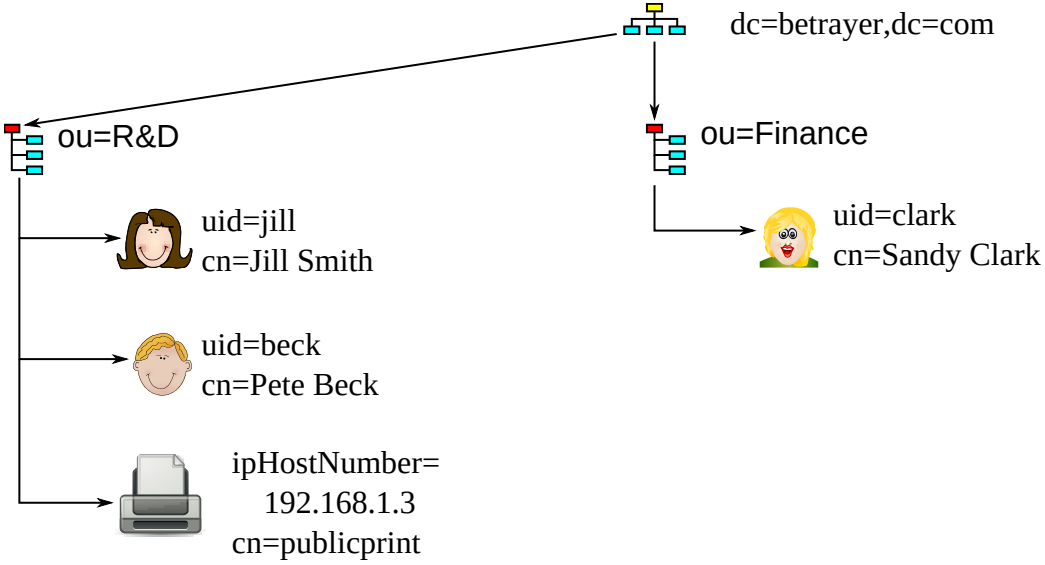
Document Information Tree (DIT)



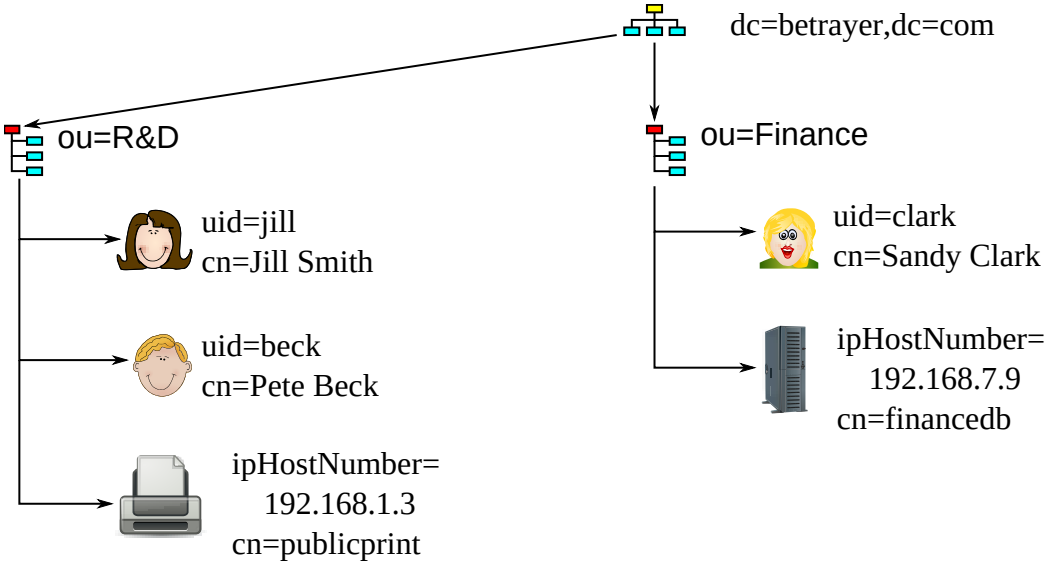
Document Information Tree (DIT)



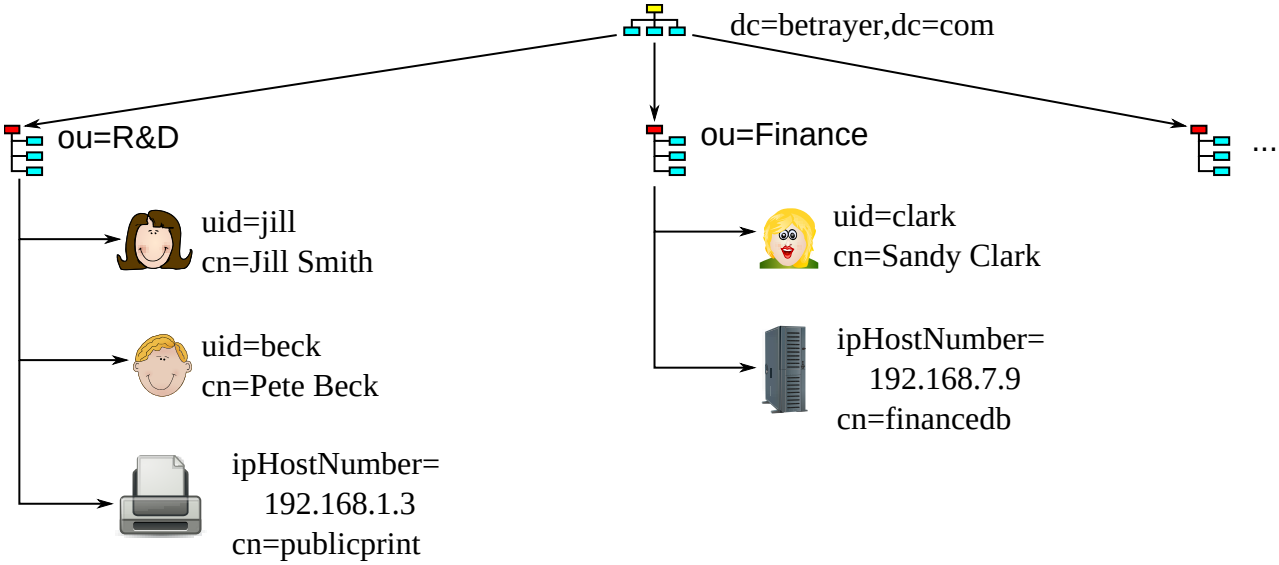
Document Information Tree (DIT)



Document Information Tree (DIT)



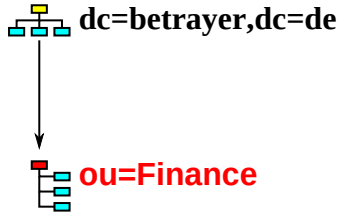
Document Information Tree (DIT)



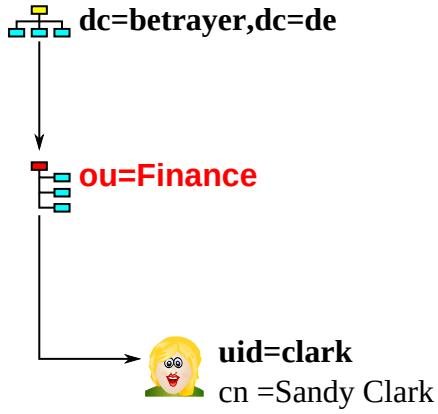
Relative and absolute DNs

dc=betrayer,dc=de

Relative and absolute DNs

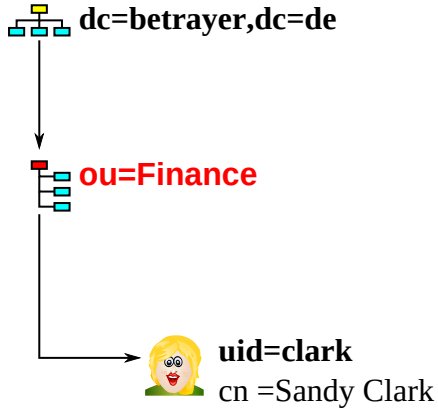


Relative and absolute DNs



Relative and absolute DNs

Relative DN values



Relative and absolute DNs

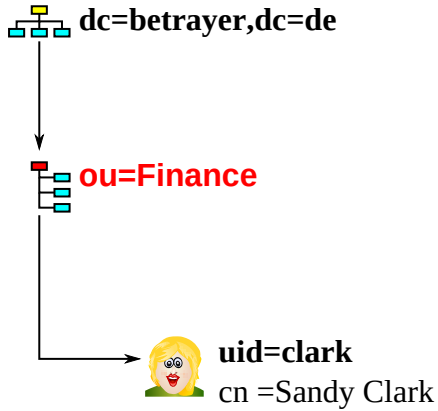
Absolute DN values

dc=betrayer,dc=de

ou=finance,dc=betrayer,dc=de

uid=clark,ou=finance,dc=betrayer,dc=de

Relative DN values



Relative and absolute DNs

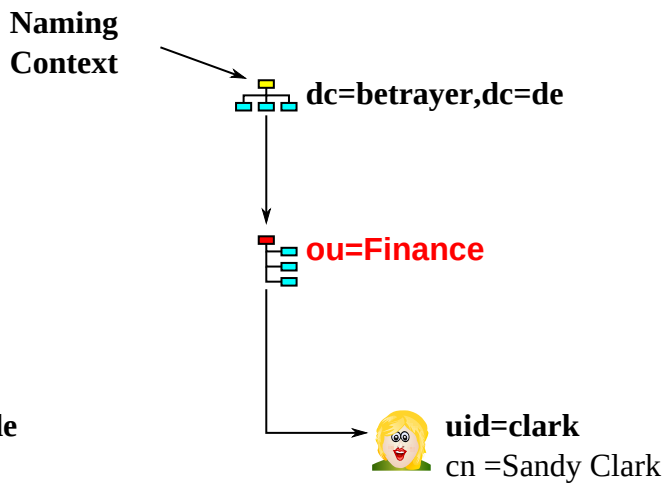
Absolute DN values

Relative DN values

dc=betrayer,dc=de

ou=finance,dc=betrayer,dc=de

uid=clark,ou=finance,dc=betrayer,dc=de



User example

```
dn: uid=clark,ou=finance,dc=betrayer,dc=de ❶
cn: Sandy Clark
homeDirectory: /home/clark
sn: Clark
uid: clark ❷
uidNumber: 21101
givenName: Sandy
loginShell: /bin/bash
mail: clark@betrayer.com ❸
mail: finance@betrayer.com
postOfficeBox: 10G
userPassword: {SSHA}noneOfYourBusiness
```

objectClass

- Structuring LDAP entry data.
- Categories:
  - Structural
  - Auxiliary
  - Abstract

objectClass clarifications

Abstract classes: To be extended by other classes

Structural classes:

- Each entry requires exactly one.
- Specify the “main” type of object.
- Must not inherit from auxiliary classes.

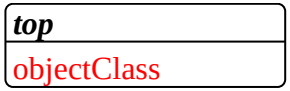
Auxiliary classes:

- Provide non-conflicting supplementary information.
- Think of (Java™) interfaces.
- Must not inherit from structural classes.

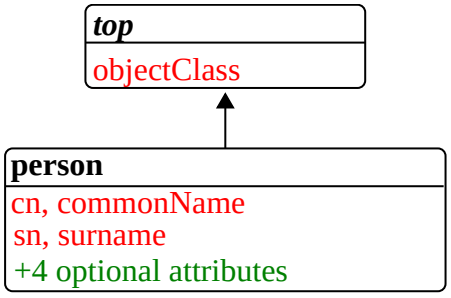
Augmenting `inetOrgPerson` by `posixAccount`

Class	Instance `uid=clark,ou=finance,dc=betrayer,dc=de`
inetOrgPerson (structural)	
sn	sn: Clark
cn	cn: Sandy Clark
...	▲
posixAccount (auxiliary)	
cn	see above ❶
gidNumber	gidNumber: 23113
homeDirectory	homeDirectory: /home/clark
uid	uid: clark
uidNumber	uidNumber: 21101
userPassword	userPassword: {SSHA}noneOfYourBusiness
	.....

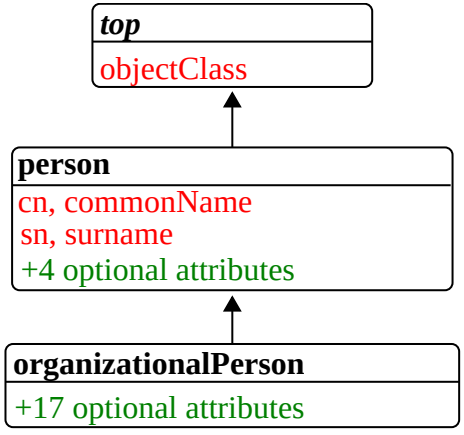
Structural objectClass definitions



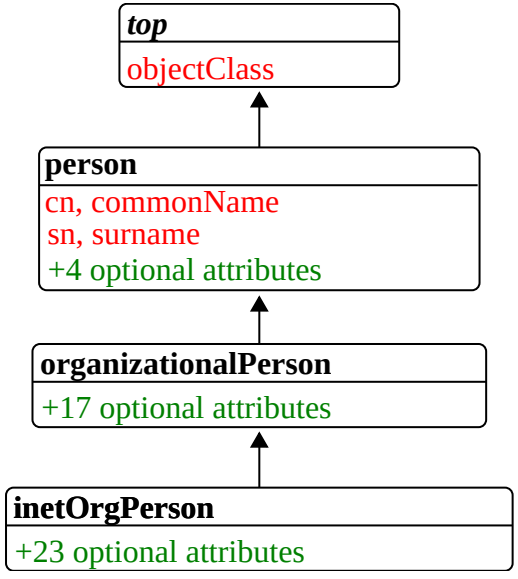
Structural objectClass definitions



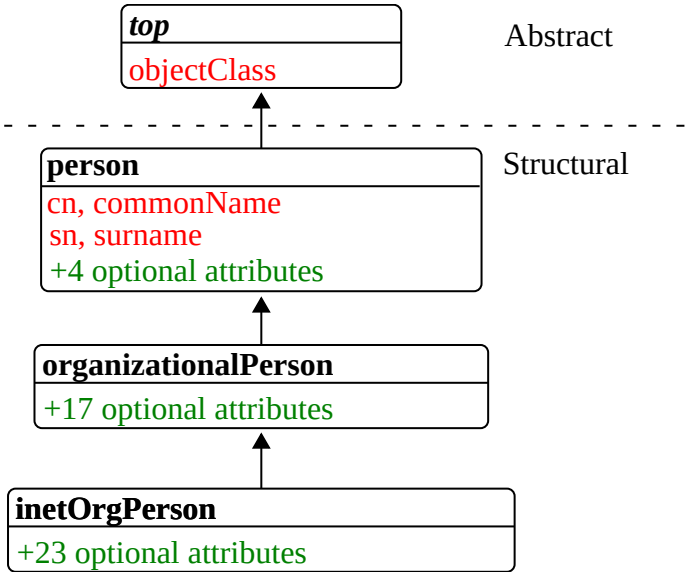
Structural objectClass definitions



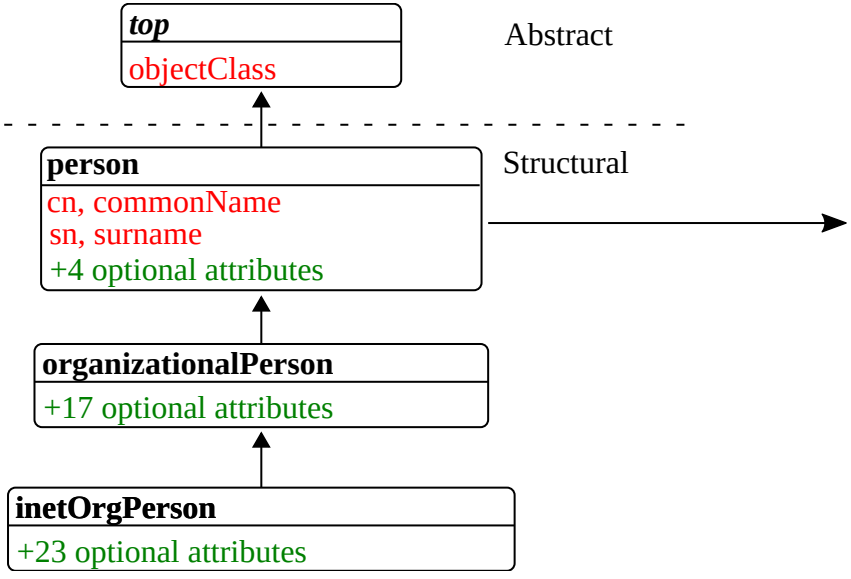
Structural objectClass definitions



Structural objectClass definitions



Structural objectClass definitions



Relational counterpart sketch:

```
CREATE TABLE person (
  cn VARCHAR NOT NULL,
  sn VARCHAR NOT NULL,
  telephoneNumber
    VARCHAR NULL,
  ...-- +3 more
)
```

Search scopes

RFC 4520 defines three LDAP search scopes:

- baseObject (`base`)
- singleLevel (`one`)
- wholeSubtree (`sub`)

Predicate based queries

RFC 4520 defines predicate based queries using RPN style:

- `(| (cn=k*) (uidNumber < 2000))`

LDAP bind types

- Anonymous bind: No user credentials.

  Note: This typically provides limited privileges.

- Simple bind: User's DN + password:

```
DN: uid=clark,ou=finance,dc=betrayer,dc=de
password: 123456789
```

LDIF exchange format

- **L**dap **D**ata **I**nterchange **F**ormat.
- Importing and exporting LDAP Data.
- Modifying existing entries (CRUD operations).
- Pure ASCII.

LDIF sample

```
dn: uid=clark,ou=finance,dc=betrayer,dc=de
objectClass: posixAccount
objectClass: inetOrgPerson
cn: Sandy Clark
homeDirectory: /home/clark
sn: Clark
uid: clark
uidNumber: 21101
givenName: Sandy
loginShell: /bin/bash
mail: clark@betrayer.com
mail: finance@betrayer.com
postOfficeBox: 10G
userPassword: {SSHA}noneOfYourBusiness
```

OpenLdap server architecture

OpenLdap server

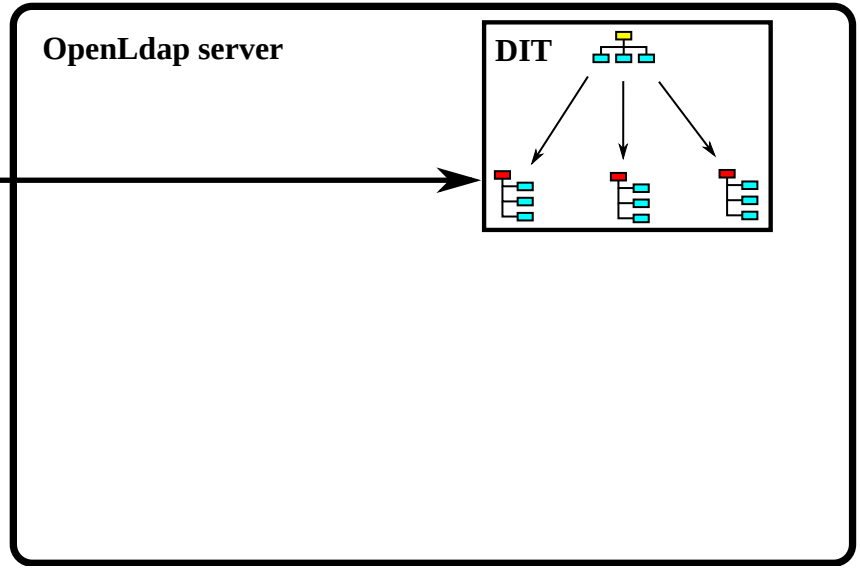
OpenLdap server architecture

dc=betrayer,dc=com

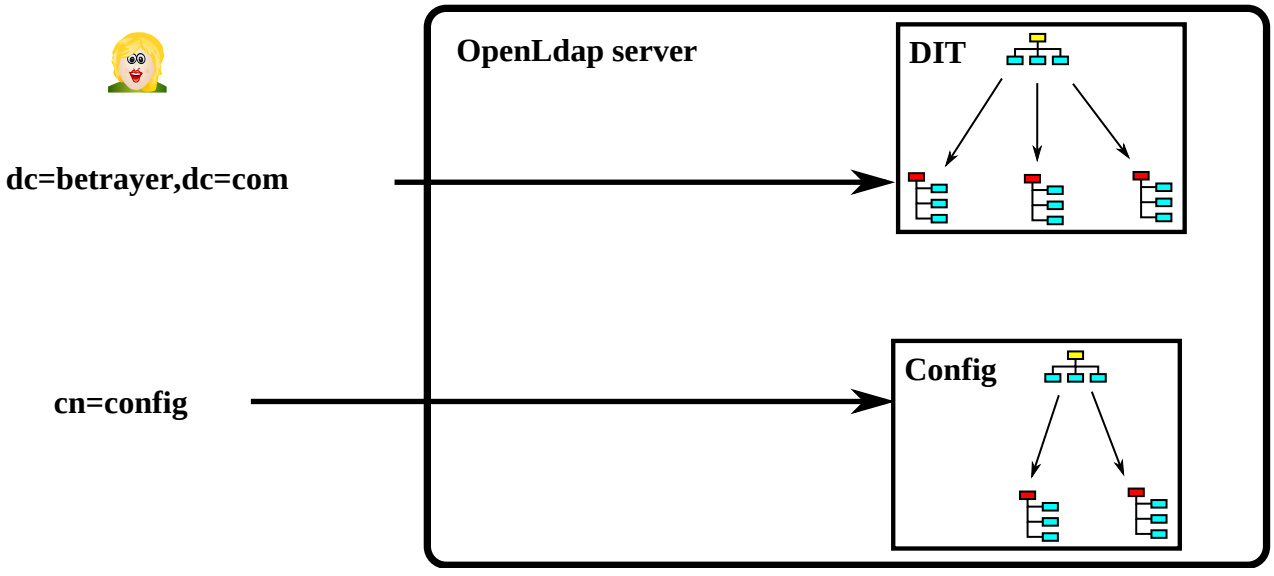
OpenLdap server

OpenLdap server architecture

dc=betrayer,dc=com



OpenLdap server architecture



An example LDAP Tree